Ноутбук — "ахиллесова пята" системы информационной безопасности

Тарас Злонов,
эксперт по ИБ,
Ника Комарова,
руководитель направления маркетинговых и PR коммуникаций,
компания Aladdin

Компания Ponemon Institute совместно с компанией Dell провела анонимный опрос более 3000 ИТ-специалистов и экспертов по информационной безопасности из США, Великобритании, Германии, Франции, Мексики и Бразилии. Согласно полученным данным исследования, три четверти респондентов сообщили, что сотрудники их компаний постоянно просматривают на проверяемых ноутбуках изображения обнаженной натуры, различные видеоролики, сайты для взрослых. Две трети опрошенных специалистов сообщили, что находят на компьютерах следы нерабочего общения с другими сотрудниками на сексуальные и иные темы, не связанные с работой. 63% ИТ-специалистов обнаружили готовые резюме и другие доказательства поиска новой работы сотрудниками.

Подобное поведение пользователей, как считают авторы опроса, свидетельствует о высоком уровне риска для корпоративных сетей, потому что доступ к сайтам для взрослых, поиск работы на подозрительных ресурсах и другие виды нецелевого использования рабочих ноутбуков могут привести к серьезным последствиям: утечкам информациии, проникновению вредоносного ПО в сеть организации.

Опрошенные респонденты сообщили, что в их организациях ноутбук в качестве основного ПК используют от 23 до 33% сотрудников. В ближайшие 5 лет респонденты ожидают увеличения этой доли до 55% в Мексике (минимальный результат), 64% в США и 65% в Германии (максимальный результат).

Для минимизации подобных рисков различные производители средств защиты предлагают свои решения. Чтобы разобраться с тем, что выбрать, давайте для начала попробуем понять, что собой представляет современный ноутбук с точки зрения организации и какие реальные угрозы для него существуют.

Под крылом самолета...

Начнем с экрана. Любопытные соседи по кафе или креслу самолета могут, конечно, оказаться злоумышленниками, но все же вероятность получения доступа к конфиденциальной информации таким образом вряд ли сколько-нибудь велика. С другой стороны, защита от посторонних глаз стоит совсем недорого: нередко сами сотрудники устанавливают защитную поляризационную пленку на экран стоимостью несколько сотен рублей. Чуть меньшая яркость экрана с лихвой компенсируется спокойным изучением годового отчета под боком самого любопытного соседа.

Другая опасность для изображения экрана монитора — побочное электромагнитное излучение (ПЭМИН). В последнее время в прессе поутих ажиотаж по поводу того, как с помощью специальной аппаратуры можно удаленно перехватить изображение с работающего экрана монитора. Отчасти это связано с тем, что тема перестала быть модной, а отчасти с тем, что излучения современных мониторов не в пример слабее тех, что излучали ЭЛТ-мониторы (на электронно-лучевых трубках) — по легенде обычная бытовая магнитола могла стать грозным оружием в руках преступников. С другой стороны, в государственных организациях, где цена информации слишком высока, до сих пор используют экранированные помещения и специальные генераторы шумов, заглушающие несанкционированные излучения компьютера. Такие приборы, кстати, довольно компактны и при высокой степени параноидальности могут быть рекомендованы к применению в том числе и частным лицам, а вот компании, пусть даже и достаточно крупной, вряд ли стоит всерьез опасаться таких каналов утечек.

Путы беспроводности

Беспроводные каналы передачи информации, в отличие от ПЭМИН, имеют достаточно высокий уровень сигнала и вполне могут использоваться для передачи данных в окружающее пространство. Знакомый радиолюбителям термин "направленность антенны" напрочь отсутствует в современных ноутбуках. На практике это означает, что передатчик WiFi одинаково сильно излучает не только в сторону WiFi-точки гостиницы, но вообще на все 360 градусов. Вот уж где настоящее раздолье любителю перехватить чужие данные. Да и сам персонал гостиницы может оказаться излишне любопытным или даже подкупленным.

К счастью, для решения этой проблемы достаточно построить VPN-канал с сетью организации — и передаваемая в эфир информация будет с большей или меньшей степенью (в зависимости от выбранных настроек) защищена. VPN-сервера и VPN-клиенты сегодня не являются редкостью — они уже не раз были подробно описаны. Не будем на них останавливаться, а упомянем лишь, что для настоящей надежности при построении удаленных соединений не рекомендуется использовать парольную защиту. Более надежным способом обеспечения безопасного доступа к информационным ресурсам является использование смарт-карт и USB-токенов для аутентификации (см. рисунок). Они не сильно утяжелят сотрудника, но существенно повысят безопасность работы не только при беспроводном доступе, но и, в целом, при подключении к сети Интернет. Вопрос контроля и разграничения доступа мы рассмотрим более детально ниже.

USB-токен для аутентификации — надежная альтернатива паролю

Об утечках через Bluetooth широкой общественности неизвестно, но, на всякий случай, можно порекомендовать изначально отказаться от моделей с этим модулем — благо для производственных задач он редко используется. Если же Bluetooth есть, и даже просто отключить его нельзя (например, производитель решил таким образом подключить мышку), то достаточно в настрой-

ках соответствующей службы отключить лишние возможности по построению сетевых соединений и приему-передаче файлов. Параноикам рекомендуется вскрыть корпус и аккуратно выпаять ненужную микросхему, а мышку заменить на проводную.

Инфракрасные излучатели и прочие экзотические передатчики ввиду их малой распространенности оставим за рамками данного обзора.

Жесткий диск: не защищен — значит уязвим

Без сомнения, самым опасным источником утечки информации является носитель, который хранит эту информацию дольше всего и в наибольшем объеме. Действительно, на экране монитора помещается одна страничка текста, а по безпроводным интерфейсам информация моет быть перехвачена лишь в момент ее передачи. Другое дело — жесткие диски. Объемы информации значительны, а срок хранения — десятки лет. Конечно, злоумышленнику потребуется физический доступ к ноутбуку, но, как было рассмотрено выше, на сегодня это не такая большая проблема. Да и выкрасть ноутбук, пожалуй, все же дешевле, чем купить аппаратуру для перехвата изображения дисплея.

Именно о защите информации на жестких дисках и пойдет речь далее.

Близнецы-братья

Сразу заметим, что несмотря на разность в физических принципах работы, с точки зрения классификации каналов утечки информации, винчестер и флэшка фактически не различаются. Даже объемы современных флэшек вот-вот приблизятся к нижней границе продаваемых жестких дисков. Это позволяет уже сейчас использовать их для загрузки операционных систем. По сути, эти устройства можно попытаться различить только способом подключения — внутренняя шина на материнской плате и USB-разъем, да и то вряд ли, ведь все больше пользователей используют внешние жесткие диски. Нахождение внутри и вне корпуса тоже плохой классифицирующий фактор: уже упоминавшаяся загрузка с внешних носителей позволяет использовать бездисковые ноутбуки. Сам же корпус ноутбука слишком непрочен, чтобы помешать желающему сделать внутренний диск внешним.

Таким образом, пожалуй, единственным фактором, определяющим способ защиты, будет наличие или отсутствие на винчестере (или флэшке) операционной системы.

Область применения

Не так давно Министерство здравоохранения и социальных служб штата Оклахома (Oklahoma Department of Human Services, DHS) объявило о краже ноутбука, содержавшего персональные данные около миллиона человек. В результате утечки пострадали обычные жители, которые получали различные государственные дотации или участвовали в госпрограммах. По данным аналитического центра Perimetrix, на украденном компьютере хранились их имена, даты рождения и адреса, а также номера социального страхования. Руководитель DHS Говард Хендрик заявил, что риск компрометации данных не очень велик, поскольку компьютер "использует систему парольной защиты".

Вполне возможно, что используемая защита действительно надежна и г-н Хендрик просто неправильно ее назвал, но на практике единственным способом защиты данных на мобильных устройствах, как известно, является шифрование. Все остальные либо слишком ненадежны, либо чрезвычайно дороги.

К выбору системы шифрования нужно подходить взвешенно. Прежде всего от таких систем требуется безупречное выполнение основной задачи — надежной защиты информации вне зависимости от того, хранится ли она на системном разделе, внешнем диске или специальном файле-контейнере.

Суть шифрования проста — преобразование информации к виду, который для стороннего наблюдателя, не знающего ключа шифрования, представляется бессмысленным набором символов. Наиболее удобным для пользователя является вариант, когда шифрование выполняется прозрачно, т.е. не нужно выполнять дополнительных действий по расшифровке файлов перед началом работы и зашифровке их при завершении. Информация всегда хранится в зашифрованном виде, а работать с ней можно после прохождения процедуры аутентификации и до выхода из системы.

Проблема защиты данных появилась не вчера и разработчики программных и аппаратных средств уже давно встраивают в свои продукты поддержку того или иного метода шифрования. Рассмотрим этот вопрос подробнее.

Встроенные средства защиты: плюсы и минусы

Практически любая современная операционная система содержит встроенную поддержку шифрования. Другой вопрос, насколько надежно предлагаемое шифрование и насколько удобно для пользователя оно реализовано? Например, в ОС Linux создать шифрованную папку и защитить ее паролем достаточно просто, более того, можно сделать шифрованным весь жесткий диск, но дружелюбных операционных систем на базе Linux, в которых комфортно работать обычному неподготовленному пользователю, пока на рынке не так много, и в большинстве случаев администратору придется все же защищать данные в среде Windows. Компания Microsoft до недавнего времени предлагала только EFS — шифрованную файловую систему, к которой было слишком много нареканий. Высказывалось даже мнение, что EFS нужна только для того, чтобы показать, что в Windows тоже есть шифрование.

Появившаяся в Windows Vista и продолжившая свое развитие в Windows технология BitLocker имеет ряд нововведений. Основное преимущество BitLocker перед конкурентами состоит в его "бесплатности". Вполне возможно, что, имея встроенное и полностью интегрированное с Active Directory ре-

шение по шифрованию данных, далеко не все пользователи платформ Microsoft будут искать ему замену.

Вместе с тем в нашей стране, в силу ряда законодательных норм, действуют ограничения как на стойкость криптографии, так и на использование TPM — аппаратных модулей доверенной загрузки. Уточним, что TPM является важнейшим компонентом технологии BitLocker — в защищенной памяти устройства, размещенного на материнской плате, сохраняется ключ шифрования, а доступ к памяти самого устройства ограничивается паролем. Без TPM действительно надежную защиту данных BitLocker обеспечить не в состоянии.

Выдвигая в качестве основных критериев высокий уровень безопасности, удобство управления и адекватную стоимость, логично остановить свой выбор на комплексном решении по шифрованию данных с централизованным управлением и резервным копированием ключевой информации. К этому стоит добавить наличие аутентификации с применением USB-ключей или смарт-карт, а также разумную стоимость.

Не так давно группа энтузиастов исследовала линейку внешних защищенных USB-дисков Staray S китайского вендора Raidon. Производитель заявлял, что все содержимое этих дисков разбивается на две части — открытую, с которой, в частности, стартовало специализированное приложение, и закрытую, доступ к которой якобы был надежно защищен вводимым в этом самом приложении паролем. На практике оказалось, что в устройствах использовалось элементарное линейное преобразование, для взлома которого потребовалось буквально несколько минут!

Защитить системный раздел

К выбору системы шифрования нужно подходить взвешенно. Прежде всего от таких систем требуется безупречное выполнение основной задачи — надежной защиты информации вне зависимости от того, хранится она на системном разделе, внешнем диске или специальном файле-контейнере.

Шифрование системного раздела — это действительно крайне удобное решение. С этой опцией не нужно заботиться о том, на каком именно диске и в какой папке пользователь размещает файлы. Если уж в метаданных документов, легально размещенных на сайтах ФБР и ракетного командования США, исследователи нашли информацию, способную помочь хакерам во взломе компьютерных сетей, то в системном реестре, кэшах браузера и логах операционной системы могут оказаться куда более значительные сведения. Шифрование отдельных или выбранных папок может быть удобно для домашнего пользователя, который самостоятельно настраивает систему шифрования и использует ее для защиты редко меняющихся объектов. Например, можно защитить папку со старыми фотографиями на внешнем диске. В организации, а также при интенсивной работе с данными, которые нужно защищать, такой подход становится слишком громоздким и неудобным.

К сожалению, при всем многообразии продуктов для защиты данных, далеко не все они корректно выполняют шифрование системного раздела, редко поддерживают спящий "режим" и шифрование дампа памяти при системном сбое. Зачастую ошибки разработчиков при реализации функций системы могут привести к полной потере всех данных. Как известно, криптографические преобразования не обратимы при отсутствии ключа шифрования. Гарантией высокой надежности системы может стать опыт вендора в разработке систем защиты информации и многолетняя история продукта — новоиспеченные продукты априори будут проигрывать тем, над которыми команда специалистов трудится более 10 лет.

Если вернуться к вопросам надежности, то важнейшим определяющим фактором, без сомнения, является алгоритм шифрования. Разработчик, как минимум, должен позаботиться о том, чтобы для защиты данных было доступно несколько алгоритмов с тем, чтобы, в зависимости от стоящих задач, можно было подобрать оптимальный. Естественно, предлагаемые алгоритмы должны быть современными. Наличие в списке алгоритмов 256-битных вариантов представляется более предпочтительным.

Доверяй, но проверяй

Вопрос обеспечения безопасного доступа к информационным ресурсам является ключевым при выборе системы защиты. Во избежание ситуации, когда человеческий фактор оказывается “ахиллессовой пятой” в системе безопасности, важно учесть критерий удобства и простоты использования. Если для доступа к шифрованным данным нужно будет вводить длинный и сложный, и что еще хуже — регулярно меняющийся пароль — то рано или поздно пользователь запишет его в легкодоступном для злоумышленика месте. С другой стороны "слабая" парольная политика таит угрозу банального взлома всей системы путем элементарного подбора. Разумным выходом, как мы уже упоминали, представляется использование аппаратных электронных USB-ключей — токенов — для аутентификации пользователя при доступе к данным.

Решения, поставляемые с токенами, стоят дороже, чем чисто программные продукты, но имеют несравнимо более высокую надежность. Кроме того, пользователю не нужно будет запоминать десятисимвольные пароли: для доступа к данным нужны два фактора — сам аппаратный ключ и ПИН-код от него, и, следовательно, можно разрешить без потери надежности более простые пароли (ПИН-коды). Любой современный токен имеет встроенное ограничение на количество попыток ввода ПИН-кода, что защищает систему от попыток перебора.

Постскриптум

Потеря ноутбука в среднем обходится компании в 50 тыс. долл. В то же время, шифрование данных позволяет снизить потери более чем на 20 тыс. долл. Этот вывод делается в отчете уже упоминавшегося Ponemon Institute. Указанная сумма ущерба включает расходы на покупку нового компьютера (1582 долл.), финансовые потери, обусловленные утратой интеллектуальной собственности (5871 долл.), а также потери, вызванные снижением продуктивности труда сотрудников (243 долл.). В сумму также включены затраты на поиск компьютера и проведение технической экспертизы (262 и 814 долл. соответственно). Затраты, которые компания несет вследствие безвозвратной утраты важной информации, составляют 80% от указанной суммы (39297 долл.). При этом замена компьютера обходится всего лишь в 2%.

Как видно, большая часть этой суммы — деньги, потерянные из-за утраты важных данных. Причем чем оперативнее сотрудник сообщает о пропаже, тем меньше расходы.

Однако такие впечатляющие цифры вовсе не повод отказаться от использования ноутбуков. Хорошая, надежная и удобная для пользователя система по шифрованию данных на мобильных компьютерах стоит гораздо дешевле.

Как справедливо заметил вице-президент Intel, генеральный директор Mobile Products Group Мули Эден (Mooly Eden): "Ноутбуки дают свободу и, кроме того, позволяют поднять производительность труда. В связи с этой тенденцией компании должны проявлять к безопасности компьютеров мобильных сотрудников большее внимание".